Homeland Security

Daily Open Source Infrastructure Report 09 December 2015

Top Stories

- Heavy flooding in Washington, Oregon, and California caused public transit delays, displaced at least 100 families, prompted officials to issue a costal hazard warning, and closed several roads December 7. – *Weather.com* (See item **5**)

- Health officials closed all food-service locations inside the Russell Investments Center in Seattle December 7 after nearly 200 people who attended a party became ill with norovirus. – *Reuters* (See item **12**)

- FireEye released a potential remediation 6 hours after Project Zero researchers reported that a remote code execution (RCE) vulnerability was found affecting FireEye's Malware Protection System (MPS). – *SecurityWeek* (See item **21**)

- Officials reported that 94 families were displaced from the Tenino Terrace apartment complex in Portland, Oregon, after the Johnson Creek flooded, spilling pollutants and chemicals December 7. – *Portland Oregonian* (See item **22**)

Fast Jump Menu

PRODUCTION INDUSTRIES

- Energy
- Chemical
- Nuclear Reactors, Materials, and Waste
- Critical Manufacturing
- Defense Industrial Base
- Dams

SUSTENANCE and HEALTH

- Food and Agriculture
- Water and Wastewater Systems
- Healthcare and Public Health

SERVICE INDUSTRIES

- Financial Services
- Transportation Systems
- Information Technology
- Communications
- Commercial Facilities

FEDERAL and STATE

- Government Facilities
- Emergency Services

Energy Sector

1. *December 7, Carlsbad Current-Argus* – (Texas) **Ramsey plant fire close to being extinguished.** Crews worked to contain a fire that continued burning inside the Ramsey Natural Gas Processing Plant in Orla, Texas, December 7 following an initial explosion and series of fires December 3 that prompted an evacuation of the plant and surrounding areas. The plant suffered extensive damage and an investigation into the cause of the explosion is ongoing.
Source: http://www.currentargus.com/story/news/local/2015/12/07/ramsey-plant-fire-close-being-extinguished/76942420/

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

2. *December 8, Military.com* – (National) **Army lifts US helicopter fleet grounding triggered by fatal crashes.** The U.S. Army announced December 7 that it ended a weeklong grounding of its stateside rotary fleet of more than 1,100 aircraft following a 5-day shutdown to review safety procedures after 3 helicopter crashes occurred within 10 days, killing 8 soldiers.
Source: http://www.military.com/daily-news/2015/12/08/army-lifts-grounding-of-us-helicopter-fleet-three-fatal-crashes.html

Financial Services Sector

3. *December 7, Las Vegas Review-Journal* – (International) **Las Vegas jury convicts two in multimillion-dollar fraud.** A Federal jury in Las Vegas convicted 2 men December 7 for their roles in an investment fraud scheme that bilked 30 investors out of $11 million between 2009 and 2011 by convincing them to invest $100,000 to $1.2 million in the fraudulent Swiss company, the Malom Group. Four other individuals were also charged in the scheme.
Source: http://www.reviewjournal.com/news/las-vegas/las-vegas-jury-convicts-two-multimillion-dollar-fraud

4. *December 7, U.S. Attorney's Office, Western District of Pennsylvania* – (International) **U.S. citizen deported from Uganda to face counterfeiting charges in western Pennsylvania.** Officials in Pennsylvania announced December 7 that a U.S. citizen was

extradited from the Republic of Uganda and charged with allegedly operating a worldwide cyber counterfeiting scheme that circulated over $1.4 million in fake U.S. Federal Reserve Notes from December 2013 – December 2014.
Source: https://www.fbi.gov/pittsburgh/press-releases/2015/u.s.-citizen-deported-from-uganda-to-face-counterfeiting-charges-in-western-pennsylvania

Transportation Systems Sector

5. *December 8, Weather.com* – (National) **Portland is under water: sewers overflow, roads flood as relentless storms hit the Northwest.** Heavy flooding in Washington, Oregon, and California caused public transit delays, displaced at least 100 families from an apartment complex in Portland, prompted officials to issue a costal hazard warning in California, and caused a rockslide to shut down U.S. Route 12 in Yakima County for several hours December 7.
   Source: http://www.weather.com/storms/severe/news/pacific-northwest-storm-impacts

6. *December 8, WCTV 6 Thomasville –* (Florida) **FHP identifies Apalachicola man killed in accident.** A portion of Coastal Highway (U.S. 98) in St. Marks was closed for several hours December 7 while officials investigated the scene of a fatal crash that killed 1 person.
   Source: http://www.wctv.tv/home/headlines/FHP-Fatal-Traffic-Crash-Shuts-Down-Coastal-Hwy-360853951.html

7. *December 8, KNTV 11 San Jose* – (International) **Paris-bound flight from SFO diverted to Montreal due to bomb threat.** An Air France flight traveling from San Francisco to Paris was diverted to Montreal, Canada December 7 after the airline received an anonymous threat. The airline cleared the plane for takeoff December 8 after nothing suspicious was found.
   Source: http://www.nbcbayarea.com/news/local/Paris-Bound-Flight-From-SFO-Diverted-to-Montreal-Officials-360891801.html

8. *December 8, Los Angeles Daily News* – (California) **Judge approves $2.4M settlement over underground storage tanks at LA airports.** The Los Angeles World Airports (LAWA) agreed to pay $2.4 million in a settlement reached with the State water board December 7 over allegations that LAWA improperly monitored underground tanks that store hazardous materials at several area airports and operated three unpermitted and unmonitored underground storage tank systems containing petroleum-based fuels at Los Angeles International Airport's burn sites. LAWA reported that the issues were corrected and removed 6 of 19 underground storage tanks and will remove several others in the next 3 years.
   Source: http://www.dailynews.com/general-news/20151207/judge-approves-24m-settlement-over-underground-storage-tanks-at-la-airports

9. *December 7, Associated Press* – (Washington) **BNSF fined $71K for late reports on oil leaks, hazardous spills along railways.** BNSF Railway was fined $71,700 by the Washington State Utilities and Transportation Commission December 7 for failing to report 14 cases of crude oil leaks and other hazardous spills along the State's railway.

Source: http://q13fox.com/2015/12/07/utc-bnsf-fined-71k-for-late-reports-on-oil-leaks-hazardous-spills-along-railways/

10. *December 7, WGHP 8 High Point* – (North Carolina) **Person killed in head-on collision on NC 68 in Guilford County.** North Carolina Highway 68 in Oak Ridge was closed for approximately 4 hours December 7 while crews cleared the scene of a fatal head-on collision involving a semi-truck and another vehicle that killed 1 person and caused a diesel spill.
Source: http://myfox8.com/2015/12/07/highway-patrol-investigating-fatal-wreck-on-nc-68-in-guilford-county/

Food and Agriculture Sector

11. *December 8, WCVB 5 Boston; Associated Press* – (Massachusetts) **80 BC students report getting sick after eating at Chipotle.** Boston College officials announced December 8 that as many as 80 students became sick after eating at a Chipotle Mexican Grill, Inc. restaurant in Brighton. The restaurant was ordered closed during the investigation into the source of the illness.
Source: http://www.wcvb.com/news/officials-trying-to-find-cause-after-30-sickened-at-chipotle/36855310

12. *December 7, Reuters* – (Washington) **Two hospitalized, nearly 200 sickened in Seattle norovirus outbreak.** Health officials closed all food-service locations inside the Russell Investments Center in Seattle December 7 after nearly 200 people who attended a party catered by California-based Bon Appetit Management Co., December 1 became ill with norovirus. The building was disinfected and authorities continue to investigate the source of the illness.
Source: http://www.reuters.com/article/us-washington-norovirus-idUSKBN0TR06I20151208

13. *December 7, San Diego Union-Tribune* – (California) **Sushi investigation nets seafood fraud convictions.** Authorities announced December 7 that eight sushi restaurants in San Diego were convicted for violating a food misbranding law after DNA lab testing found that the businesses were advertising the sale of lobster rolls that contained crawfish and pollack instead of lobster. The owners and operators of the restaurants pleaded guilty to violating the State law and agreed to pay over $19,000 in collective fees and investigation costs.
Source: http://www.sandiegouniontribune.com/news/2015/dec/07/phony-lobster-rolls-nets-fraud-pleas/

Water and Wastewater Systems Sector

14. *December 7, Kitsap Sun* – (Maine) **Bangor sewage spill dumps 12,000 gallons.** Officials reported that approximately 12,000 gallons of sewage spilled into U.S. Naval Base Kitsap-Bangor’s stormwater collection system December 7. No health advisories were issued due to the discharge point into Hood Canal being closed to public access.
Source: http://www.kitsapsun.com/news/local-news/bangor-sewage-spill-dumps-

12000-gallons_37802813

For another story, see item **8**

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

15. *December 8, Columbus Dispatch* – (Ohio) **College of Wooster cancels classes after two bomb threats.** Classes at the College of Wooster in Ohio resumed December 8 after two bomb threats prompted the evacuation of buildings and the cancellation of classes December 7. Police searched the campus following the threats and provided additional security at the school.
Source: http://www.dispatch.com/content/stories/local/2015/12/08/college-of-wooster-cancels-classes-after-two-bomb-threats.html

16. *December 8, WJAX 47 Jacksonville* – (Florida) **Officials investigating bomb threat at Orange Park High; classes canceled Tuesday.** Orange Park High School in Clay County was closed December 8 due to an emailed bomb threat received by a school administrator. No suspicious items were found after police searched the campus.
Source: http://www.actionnewsjax.com/news/news/local/orange-park-school-closed-due-bomb-threat/npfDK/

17. *December 7, U.S. Securities and Exchange Commission* – (International) **SEC: lawyers offered EB-5 investments as unregistered brokers.** The U.S. Securities and Exchange Commission announced December 7 that at least 8 lawyers across the U.S. were charged with offering EB-5 investments as unregistered brokers through the government’s EB-5 Immigrant Investor Program, including one New York-based lawyer who sold the investments to more than 100 investors and defrauded clients by failing to disclose the commissions received on the investments. Seven lawyers and their firms agreed to cease and desist from acting as unregistered brokers and agreed to pay penalties.
Source: http://www.sec.gov/news/pressrelease/2015-274.html

For another story, see item **2**

Emergency Services Sector

Nothing to report

Information Technology Sector

18. *December 7, Softpedia* – (International) **Malware steals iOS and BlackBerry backups via infected PCs.** Palo Alto Networks released a report stating that many mobile backup tools lack secure encryption protocols, which can allow attackers to

steal local mobile backup data and sensitive information from infected Apple Mac and Microsoft Windows computers, and discover and extract Apple iOS and Microsoft BlackBerry backup files via 6 trojan families that use the BackStab attack technique. Security researchers advised users to use backup tools that supports encryption, to maintain routine updates to their mobile operation system (OS), and to use an antivirus product, among other recommendations.
Source: http://news.softpedia.com/news/malware-steals-ios-and-blackberry-backups-via-infected-pcs-497244.shtml

19. *December 7, SecurityWeek* – (International) **Rootnik trojan modifies legitimate root tool to hack Android devices.** Researchers at Palo Alto Networks discovered a new trojan, dubbed Rootnik, that uses the Root Assistant utility to gain root access on Android devices, which can allow attackers to download executable files from remote servers for local execution; steal Wi-Fi passwords, keys, Service Set Identifiers (SSID), and Basic Service Set Identifiers (BSSID); and harvest victims' private information. The trojan can infect computers by being embedded on copies of legitimate applications including Wi-Fi Analyzer, Open Camera, Infinite Loop, and HD Camera, among other tools.
Source: http://www.securityweek.com/rootnik-trojan-modifies-legitimate-root-tool-hack-android-devices

20. *December 7, Softpedia* – (International) **Google patches Android for more bugs in its December security bulletin.** Google released security updates addressing 19 flaws in Nexus devices for its Android builds LMY48Z and later, and Android Marshmallow including a critical security vulnerability that can enable a remote code execution (RCE) to affect devices through email, web browsing, and Multimedia Messaging Service (MMS) when processing media files, and as well as a critical severity flaw affecting Android's Skia graphics engine (RCE), the display driver, and an elevation of privileges in the kernel itself.
Source: http://news.softpedia.com/news/google-patches-android-for-more-bugs-in-its-december-security-bulletin-497259.shtml

21. *December 7, SecurityWeek* – (International) **FireEye patches critical flaw found by Google researchers.** Researchers from Project Zero discovered and reported that a remote code execution (RCE) vulnerability was found affecting FireEye's Malware Protection System (MPS) including its Network Security (NX), Email Security (EX), Malware Analysis (AX), and File Content Security (FX) products. FireEye released an automated remediation to customers 6 hours after notification and mitigated potential customer exposure.
Source: http://www.securityweek.com/fireeye-patches-critical-flaw-found-google-researchers

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: http://www.it-isac.org

Communications Sector

Nothing to report

Commercial Facilities Sector

22. *December 8, Portland Oregonian* – (Oregon) **SE Portland apartment complex residents evacuate as flooding precaution.** A Portland Fire & Rescue official reported December 7 that 9 apartment buildings were affected and up to 94 families were displaced from the Tenino Terrace apartment complex following voluntary evacuations after the Johnson Creek flooded, spilling pollutants and chemicals. Officials reported that water levels were as high as 12 inches and may have leaked into the apartments. Source: http://www.oregonlive.com/portland/index.ssf/2015/12/se_portland_low-income_housing.html

23. *December 6, Harrisburg Patriot-News* – (Pennsylvania) **Man accused of causing $300K damage to Williamsport motel.** A Lycoming County man was arrested and charged for causing or risking a catastrophe and criminal mischief at the Holiday Inn Express in Williamsport, Pennsylvania, after allegedly breaking a sprinkler head in a third-floor room, forcing the evacuation of the hotel, and causing an estimated $300,000 in damages December 5.
Source:
http://www.pennlive.com/news/2015/12/man_accused_of_causing_300000.html

For another story, see item **5**

Dams Sector

24. *December 8, Jamestown Sun* – (North Dakota) **Releases from dams temporarily shut down.** Officials reported December 8 that releases from the Jamestown and Pipestem dams in North Dakota were temporarily shut down due to the reduced river levels caused by the releases.
Source: http://www.jamestownsun.com/news/local/3898798-releases-dams-temporarily-shut-down

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.